



102 South Eastern Street • Sanborn, IA 51248

712-930-5593
877-537-5593
fax: 712-930-5595
tca@tcaexpress.net

02/06/2008

Received & Inspected

FEB 11 2008

FCC Mail Room

DOCKET FILE COPY ORIGINAL

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

RE: EB Docket No. 06-36
Annual CPNI Certification for Year 2007

Dear Ms. Dortch:

In accordance with Public Notice DA 08-171, issued on January 29, 2008, attached is the annual CPNI certification filing for the year of 2007 for The Community Agency.

Sincerely,

DJ Weber
General Manager

Attachment

cc: Federal Communications Commission (*two copies*)
Enforcement Bureau
Telecommunications Consumers Division
445 12th Street, SW
Washington, D.C. 20554

Best Copy and Printing, Inc. (*one copy*)
445 12th Street
Suite CY-B402
Washington, D.C. 20554

No. of Copies (incl. 044
LBI AV005



102 South Eastern Street • Sanborn, IA 51248

712-930-5593
877-537-5593
fax: 712-930-5595
tca@tcaexpress.net

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Received & Inspected

FEB 11 2008

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2007

Date filed: 02/06/2008

Name of company covered by this certification: The Community Cable Television Agency of O'Brien County

Form 499 Filer ID: 821250

Name of signatory: DJ Weber

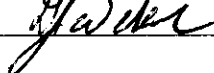
Title of signatory: General Manager

I, DJ Weber, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed 

ATTACHMENT



102 South Eastern Street • Sanborn, IA 51248

712-930-5593
877-537-5593
fax: 712-930-5595
tca@tcaexpress.net

Received & Inspected

FEB 11 2008

FCC Mail Room

Customer Proprietary Network Information (CPNI)

Certification Filing

for

**The Community Agency
102 South Eastern Street
Sanborn, Iowa 51248**

In accordance with 47 CFR § 64.2009(e), DJ Weber, General Manager for The Community Agency ("TCA"), hereby certifies that he has personal knowledge that TCA has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules (47 CFR §§ 64.2001 *et seq.*).

Attached to this Certificate is documentation describing how the procedures used by TCA ensure compliance with the CPNI rules.

I hereby certify that the information contained in this Certificate and the attached documentation is accurate and complete to the best of my knowledge, information and belief.

Signed:



Printed Name:

DJ Weber

Title:

General Manager

Date:

02-06-2008

Attachment

**Customer Proprietary Network Information (CPNI)
Documentation of Operating Procedures**

for

**The Community Agency (TCA)
102 South Eastern Street
Sanborn, Iowa 51248**

- CPNI rules are reviewed on a regular basis with employees. Employees with access to CPNI have been trained on when they are, and are not, authorized to use CPNI.
- TCA has a defined disciplinary process in place for violations and for improper use of CPNI.
- A process that meets the notice requirements of the rules has been developed for notifying customers of their CPNI rights and for requesting approval to use CPNI via the opt-out method.
- Since TCA uses the opt-out method, it provides CPNI notification to customers every two years. TCA will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly.
- A field on the customer's account record is noted to clearly show the CPNI approval or denial status for the account.
- TCA retains CPNI notification records for a minimum of one year.
- TCA has established a process for maintaining a record of any marketing campaign of its own or of its affiliates that uses the CPNI of its customers. Specific details of the campaign will be maintained on a spreadsheet and will be retained for a minimum of one year.
- Management must approve all sales and marketing campaigns. TCA has established a supervisory review process for any outbound marketing efforts to ensure that supervisory approval has been obtained for any proposed outbound marketing.
- TCA will not provide CPNI to third parties without the customer's affirmative approval via the opt-out process.



What is CPNI?

CPNI stands for Customer Proprietary Network Information

The *Gist* of CPNI:

- Protect the customer's privacy
- Market products and services within the existing customer relationship
- Do not use customer information to *target* customers
- Do not give customer information to other companies

Types of CPNI:

Call Detail Records

- Require greatest protection of privacy

Purchases

- LD PIC codes, video, Internet, wireless, features

General Account Information

- Name, address

Acceptable uses of CPNI

- Exchange of customer information for the purpose of inter-carrier billing
- Marketing of services within an existing customer relationship
- Mass Marketing such as bill notices, bill inserts, direct mail, in-house telemarketing, newsletter articles, advertising, signage
- Law enforcement
- Directory listings
- Service provisioning by independent contractors (overbuild projects)
- In-house mailings
- Provisioning of customer service, products and services (cable modems, etc)
- Protecting telco property (peds, boxes on outside of homes)

Restrictions of CPNI

- Selling or distributing of CPNI to a third party without customer approval
- Selling or distributing CPNI to a joint-venture partner or independent contractor without the customer's express permission (opt-in)
- Win-back campaigns that use information about a customer's relationship with a competitor to target that customer.
- Targeted-marketing without giving the customer an opt-out opportunity
- Discussing Call Detail Records without a password
- Providing CPNI to mail houses, telemarketers, or direct mailing firms (data brokers)



MARKETING/SALES

****CPNI impacts all employees that have access to customer records including customer service, sales, marketing, accounting, and install and repair staff.**

Marketing and CPNI

- Review ALL marketing efforts with the CPNI Compliance Officer
- Conduct as much mass marketing as possible
- Avoid target mailings. When targeting, observe the rules.

Telemarketing:

- If conducted in-house, it requires no sharing of CPNI with a third party or independent contractor
- Do NOT give target telephone numbers to telemarketing firms
- It is OK to give ALL phone numbers to telemarketing firms

Winbacks:

- It is OK to generate a list of disconnected customers and attempt to win-back.
- It is NOT OK to use port requests or cancellation codes to target competitors' customers

Websites:

- General Information on the website is not targeted and is OK.
- Account information must be password protected



Opt-in and Opt-out forms

Opt-in: Express written consent to receive marketing materials and sales communications about products and services outside the customer relationship or express written consent to share customer information with third parties, joint venture partners, and independent contractors.

TCA will not be using the Opt-In process.

Opt-out: Express written consent to be excluded from marketing materials and sales communications about products and services outside the existing customer relationship.

Opt-Out Process

- Mail form to all customers notifying them that “from time to time TCA may use your account information to promote additional products and services available from us.”
- Provide the customer the option of “opting out” by signing and returning the opt-out form, or a request can be made verbally.
- Must allow 32 days to receive opt-out forms
- Note the customer records of each opt-out
- Screen opt-outs from all future *targeted* marketing.
- Secure and store opt-out requests in the TCA CPNI files.
- New Customers: Opt-out notice will be sent after 1st month of service (run a report at the end of each month and send notification letter.) Or notification can be given to customer at time of set up.



Bill Notification

New customers will be signed up for CPNI at the application process. Existing customers will be notified every 2 years.

The Community Agency (TCA) respects your privacy and observes the privacy rules established by the Federal Communications Commission, the State Public Utility Commission and other telecom oversight agencies.

TCA will never sell your account information or provide details of your telephone calls to other parties, unless required by law enforcement.

From time to time, we would like to notify you of additional products available from us outside the existing business relationship we have with you. For example, if you have our local phone service, you may be interested to learn about specials on our cable and wireless services. However, you have the right to be excluded from these marketing campaigns.

If it is acceptable to receive information about additional products and services, you need to do nothing. However, if you prefer to be excluded from these marketing efforts, please call our office at 712.930.5593, and we will screen you from all targeted marketing programs for the next two years.

Thank you for being a TCA customer.



CUSTOMER SERVICE

CPNI in Everyday Operations

Customer Service—5 things to remember

1. Authenticate **every** customer
2. A password is **required** for Call Detail Records
3. Check customer's opt-out status
4. Ask permission to discuss products and services (“while I have you on the phone...”)
5. Aggressively upsell

Technicians-2 things to remember

1. Sell within existing customer relationship
2. Or, ask permission to discuss additional products and services
“I know I’m here to fix your phone service, but may I tell you about some new services we offer?”



Customer Authentication and Password Procedures

Customer Authentication

Every customer is required to be authenticated before details on the account are discussed.---This is to prevent pretexting. **Pretexting** is when an imposter contacts the telephone company claiming to be a customer in order to obtain call detail records or account information.

Customer Authentication Script:

To establish a password:

“I’d be happy to help you. Could you please verify the name on your account? Could you please confirm your average monthly bill?—The Federal Communications Commission now requires us to use passwords to access your account. At this time, I would like to set up a password to further protect your privacy. Could you please give me a password you would like to use on your account? We’d also like to establish a backup question.

Back-up Questions

The following questions will be used as the back-up question. The customer needs to answer only one.

- 1) What are the last 4 digits of your social security number?
- 2) What is your mother’s maiden name?
- 3) What is your childhood street name?

(If customer declines to establish a password): “I can understand that you do not want to track a password. To provide your account information, I can call you back at the telephone number we have associated with your account or you can stop by the office and present a government-issued ID, such as a driver’s license, to receive the information.”

If password is already established:

“I’d be happy to help you. Could you please verify the name on your account? Could you please verify the password on your account?”



Password Procedures

Passwords must be used to share call detail records, although TCA will obtain a password for all account information. Employees are forbidden from supplying call detail records to a customer making an in-bound call to the office, even if the caller ID indicates that the customer is calling from the telephone number of record.

If the customer is unable to supply the password or refuses to establish a password, the employee may share call detail records by:

1. Calling the customer back at the telephone number of record
2. Mailing or emailing the call detail record to the address (physical or email) of record
3. Confirming the customer's identity in person with a valid, government-issued ID

****If the customer supplies the call detail record for a particular call in question, the employee may confirm the call detail record, but only for that call. Other call detail records may not be supplied without a password, or without the customer first providing the information.**

The employee can help the customer remember passwords with back-up questions that are not based on readily available information such as social security number, childhood pet, etc. ---**However, if these questions are used to prompt the customer's memory, the FCC requires the phone company to provide notification to the address of record that the back-up questions were used to gain account access.**

How to establish a password:

1. Call the customer at the telephone number of record or authenticate the customer without the use of readily available information or account information.
2. Have the customer select a password and establish a back-up question
3. Store the password with the customer's account
4. Provide online option for online billing, if applicable

The following questions will be used as the back-up question. The customer needs to answer only one.

- 1) What are the last 4 digits of your social security number?
- 2) What is your mother's maiden name?
- 3) What is your childhood street name?



Notification of Account Change

The customer must receive a written notification within 48 hours of the following account changes:

- Email address has been added, altered, or deleted
- Hints and/or answers have been added, altered, or deleted
- Password has been added, altered, or deleted
- Name and address has been changed
- Security questions used for authentication

(THIS NOTIFICATION LETTER IS AVAILABLE ELECTRONICALLY ON MARTINS)

Dear Customer,

Per FCC rules, telecommunications companies are required to provide notice to customers when your account is accessed or certain changes are made to your account. The following is what changes you have requested for the telephone number 999.9999 on 12/12/07.

Please verify for accuracy if you did not request this change, or if you feel a security violation has occurred without authorization, please call our office at 111.1111.

(Telephone Company)



UPSELLING

When upselling use the “safety net” approach by asking permission to review the customer’s account information and discuss additional products and services.

Safety Net Example:

“May I have permission to review your account and discuss services you might not currently be receiving from us?”

Other upselling examples:

“I see that you have caller ID. Did you know that with voicemail and call waiting, you can see who’s calling when you’re on the line, and let it ring to voicemail?”

“Would you like to add a premium channel package to your order?”

“I notice that you’re using dial-up Internet, have you heard about our specials on High Speed Internet?”



UPSELLING

Already Purchase and Calling About	OK to Sell	Outside of Existing Customer Relationship
Local Exchange	Calling features, Second Lines, CPE, Key Systems	Long Distance, VoIP, High-speed Internet, Video, Wireless
Long Distance	More Minutes, Alternative Long Distance Plans, Unlimited Switched Long Distance	Local Voice, VoIP, High-speed Internet, Wireless, Video
Dial-up Internet	High-speed Internet*, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage	Local Voice, Long Distance, VoIP, Video, Wireless
High-speed Internet	VoIP, Greater Bandwidth, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage	Local Voice, Long Distance, Video
Wireless	Handsets, Expanded Service Plans, Accessories, Additional Users, Data, Text Messaging, Minutes of Use, Wireless Broadband	Local Voice, Long Distance, Video
Video	Premium Channels, DVR, VoD, HD, Digital Tiers, CPE, High-speed Internet*, Pay-per View	Local Voice, Long Distance
Triple Play	VoIP, Premium Channels, DVR, VoD, HD, Digital Tiers, CPE, High-speed Internet*, Pay-per-view, Greater Bandwidth, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage, Calling Features, Second Lines, CPE, Key Systems	Wireless



Reporting Procedures for CPNI Violations and Breaches

- Notification to Law Enforcement:
- Notify Law Enforcement within 7 business days by electronic notification through the central reporting systems of the United States Secret Service (USSS) and the FBI
- Unless requested otherwise, after 7 days of notifying law enforcement, notify the customer of the CPNI breach
- Maintain records of any discovered breaches, notifications, and law enforcement response for 2 years. Include the date of discovery, date of law enforcement notification, detailed description of the CPNI that was breached, and circumstances of the breach.

****Law enforcement may request a delay in customer notification in order to investigate the CPNI breach. TCA will observe law enforcements requests, unless there is an urgent need to notify the customer to avoid immediate and irreparable harm. All requests by law enforcement to delay customer notification should be thoroughly documented.**



Employee Disciplinary Procedures

Employees might unintentionally violate CPNI rules by mentioning a product or service outside the existing relationship or by targeting a mailing without the Compliance Officer's review. The FCC requires carriers to adopt disciplinary actions for all CPNI violations, whether intentional or unintentional.

Unintentional Violations:

Violation: Retrained and recertified

Intentional Violations:

For intentional violations, such as distribution of CPNI to third parties for financial gain, to harm the company, or to harm the customer, the breach will be reported and the employee will be terminated.



Section 222 of the 1996 Telecom Act

CPNI

Section 222 of the Telecom Act

“SEC. 222. PRIVACY OF CUSTOMER INFORMATION.

“(a) IN GENERAL.—Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

“(b) CONFIDENTIALITY OF CARRIER INFORMATION.—A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

“(C) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION.—

“(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall use only, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

“(2) DISCLOSURE ON REQUEST BY CUSTOMERS.—A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

“(3) AGGREGATE CUSTOMER INFORMATION.—A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or person on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.



“(d) EXCEPTIONS.—Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

“(1) to initiate, render, bill, and collect for telecommunications services;

“(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

or

“(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service.

“(e) SUBSCRIBER LIST INFORMATION.—Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under non discriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

“(f) DEFINITIONS.—As used in this section:

“(1) CUSTOMER PROPRIETARY NETWORK INFORMATION.—The term ‘customer proprietary network information’ means—

“(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

“(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

“(2) AGGREGATE INFORMATION.—The term ‘aggregate customer information’ means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

“(3) SUBSCRIBER LIST INFORMATION.—The term ‘subscriber list information’ means any information—

“(A) identifying the listed names of subscribers of a carrier and such subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

“(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.”



CPNI Employee Certification

I, the undersigned, hereby acknowledge receiving and reviewing TCA CPNI Rules and Policies. I have completed the training coordinated by the TCA Compliance Officer. I further understand that I am responsible for understanding and observing TCA's CPNI policies and the rules established by the Federal Communications Commission and the Iowa Public Utilities Commission.

Finally, I accept responsibility for any violations of CPNI and the rules and understand the disciplinary procedures in place at TCA, which include termination.

Name _____

Position _____

Date CPNI Manual Received _____

Date of CPNI Training _____

Signature _____ Date _____

Witnessed by the CPNI Compliance Officer

Printed Name _____

Signature _____ Date _____

****COPY FOR YOUR RECORDS** **KEEP IN BOOKLET****



Name and Contact Information of the CPNI Compliance Officer

Contact Information:

DJ Weber
102 Southeastern St.
PO Box 489
Sanborn, Iowa 51248

Duties of the Compliance Officer:

- This person is the central point of contact for employee, agents (attorneys, contractors, consultants, agents, vendors) and customers regarding the company's CPNI responsibilities
- Maintains and secures the company's CPNI files
- Tracks all customer CPNI complaints for one year
- Tracks all breaches of CPNI rules for two years
- Reviews and documents company use of CPNI



FCC CPNI Rules

Complying with the FCC's CPNI rules is a seven step process:

- 1) Designate a Compliance Officer
- 2) Train and certify employees on CPNI requirements
- 3) Notify customers of any account changes
- 4) Notify law enforcement and customers of any unauthorized disclosure of CPNI
- 5) Establish disciplinary procedures for employee violations of CPNI rules
- 6) Take measures to discover and protect against pretexting and unauthorized disclosures of CPNI
- 7) File annual certification by March 1

1) Designate a Compliance Officer

- Central point of contact for employees, agents (attorneys, contractors, consultants, vendors) and customers regarding the company's CPNI responsibilities
- Maintains and secures the company's CPNI files
- Tracks all customer CPNI complaints for one year
- Tracks all breaches of CPNI rules for two years
- Reviews and documents company use of CPNI

2) Train and certify employees on CPNI requirements

All employees and agents with access to CPNI must:

- Receive and read the company's CPNI manual
- Sign the company's CPNI Policy Acknowledgment

Attend group or private training, supervised by the CPNI Compliance Officer

3) Notify customers of any account changes

*Customers must be notified immediately by mail to the address of record, or by voicemail, or text message to the telephone number of record, upon the following:

- A new password is created or changed
- The address of record is changed
- The online account of record is changed
- Back-up questions are used to re-issue a lost or forgotten password
- A security breach occurs



4) Notify law enforcement and customers of any unauthorized disclosure of CPNI

- Notify law enforcement within seven business days by electronic notification through the central reporting systems of the United States Secret Service and the FBI.
- Unless requested otherwise, after seven business days of notifying law enforcement, notify the customer of the CPNI breach
- Maintain records of any discovered breaches, notifications, and law enforcement response for two years. Include date of discovery, date of law enforcement, detailed description of the CPNI that was breached, and circumstances of the breach

5) Establish disciplinary procedures for employee violations of CPNI rules

- Reprimand
- Retrain
- Re-certify
- Escalated disciplinary actions for repeat offenses
- Intentional distribution of CPNI to other parties to harm the company or for personal gain—termination

6) Take measures to discover and protect against pretexting and unauthorized disclosures of CPNI

- Guard against pretexting with measures beyond CPNI requirements, but consistent with Section 222, such as encryption and audit trails
- Detect pretexting
- Document actions

7) File annual certification by March 1

- Complete EB Docket No. 06-36
- Include explanations of any actions taken against data brokers
- Include a summary of all customer complaints
- File on or before March 1



CERTIFICATION OF CPNI FILING

Section 65.2009(e) of FCC Rules

EB-06-TC-060

EB DOCKET NO. 06-36

I hereby certify that I am an Officer of The Community Agency.

I have personal knowledge that the Company (and its affiliates) established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of Part 64 of the Federal Communications Commission's Rules (47 C.F.R. 64.2001 through 64.2009). The attached statement of CPNI Compliance explains how the Company's operating procedures ensure that it is in compliance with the foregoing FCC rules.

I am making this certification for the year _____.

Signature

Printed Name

Office Held

Date